

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
29 April 2004 (29.04.2004)

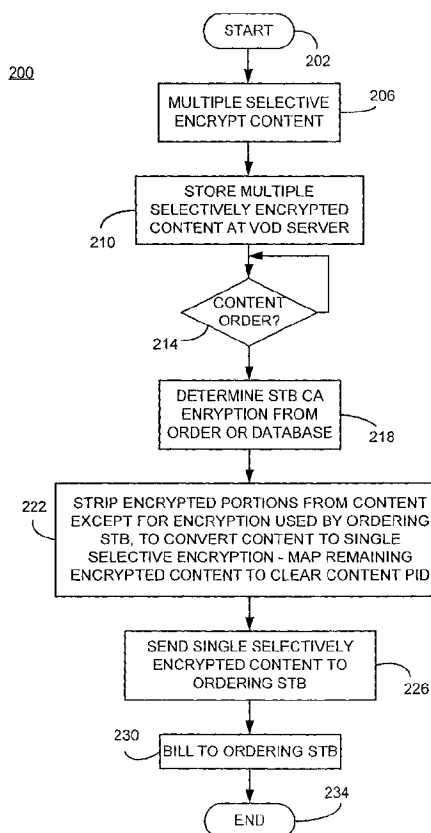
PCT

(10) International Publication Number  
**WO 2004/036892 A2**

- (51) International Patent Classification<sup>7</sup>: **H04N** (72) Inventor: CANDELORE, Brant, L.; 10124 Quail Glen Way, Escondido, CA 92029-6502 (US).
- (21) International Application Number: PCT/US2003/027775 (74) Agents: KANANEN, Ronald, P. et al.; RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036 (US).
- (22) International Filing Date: 8 September 2003 (08.09.2003) (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (25) Filing Language: English (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IJU, IE, IT, LU, MC, NL, PT, RO,
- (26) Publication Language: English
- (30) Priority Data:  
60/409,675 9 September 2002 (09.09.2002) US  
10/273,903 18 October 2002 (18.10.2002) US  
10/274,084 18 October 2002 (18.10.2002) US  
10/274,019 18 October 2002 (18.10.2002) US  
10/273,905 18 October 2002 (18.10.2002) US
- (71) Applicant: SONY ELECTRONICS INC. [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

[Continued on next page]

(54) Title: SELECTIVE ENCRYPTION FOR VIDEO ON DEMAND



(57) Abstract: A video on demand (VOD) method, consistent with the invention involves storing multiplesselective encrypted VOD content on a VOD server; receiving an order for the VOD contentspecifying delivery to a target decoder; determining what CA encryption system is associated with the order; stripping all encrypted segments from the multiple selectively encrypted contentthat are not associated with the order to produce single selectively encrypted VOD content tothe target decoder. The multiple selectively encrypted VOD content can be created by examining unencrypted data representing digital content to identify segments of content for encryption; encrypting the identified segments fo content using a first encryption method associated with a first conditional access system to produce second encrypted segments; and replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, to produce the multiple selectively encrypted VOD content.



SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

- *without international search report and to be republished upon receipt of that report*

1

2

3

4

5

6

7

8

**SELECTIVE ENCRYPTION FOR VIDEO ON DEMAND**

9

10

11

12

13

**CROSS REFERENCE TO RELATED DOCUMENTS**

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

This application is a continuation-in-part of U.S. patent applications serial number 10/273,905, filed October 18, 2002 to Candelore et al., entitled "Video Slice and Active Region Based Dual Partial Encryption", serial number 10/273,903, filed October 18, 2002 to Candelore et al., entitled "Star Pattern Partial Encryption", serial number 10/274,084, filed October 18, 2002 to Candelore et al., entitled "Slice Mask and Moat Pattern Partial Encryption", and serial number 10/274,019, filed October 18, 2002 to Candelore et al., entitled "Video Scene Change Detection", which are hereby incorporated by reference.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/409,675, filed September 9, 2002, entitled "Generic PID Remapping for Content Replacement", to Candelore and U.S. Provisional Application serial number 60/351,771, filed January 24, 2002, entitled "Method for Allowing Multiple CA Providers to Interoperate in a VOD Delivery System and Content Delivered on Package Media" to Candelore. These applications are also hereby incorporated by reference herein.

**COPYRIGHT NOTICE**

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

**FIELD OF THE INVENTION**

This invention relates generally to the field of video on demand (VOD). More particularly, this invention relates to a multiple encryption method and apparatus particularly useful for multiple encrypting digitized video on demand programming.

**BACKGROUND OF THE INVENTION**

Video On Demand (VOD) is becoming a service which cable operators now consider to be a mandatory service as much as subscription and impulse pay-per-view (IPPV). But, VOD is different from broadcast services in that content is statically stored on VOD servers (often at the cable hubs), and is delivered to a specific subscriber upon receipt of a specific request by that subscriber.

VOD servers are often located at cable hub facilities. Hubs are located out in the local neighborhoods and serve a subset of perhaps about 80,000 subscribers. By locating the VOD system at the hub level, use of bandwidth is more efficient since customers in different hubs can use the same spectrum. As a point of contrast, subscription and IPPV content is generally scrambled at a Master Headend and delivered to the hubs for distribution.

There are currently two major VOD service providers in the cable industry. In one, content is stored pre-encrypted on hard drives in the VOD server. The keys used to encrypt the content do not change from month-to-month, however,

1 the entitlement control messages (ECMs) used to derive those keys to enable  
2 the conditional access (CA) system are updated every month. In the second  
3 VOD system, content is stored in-the-clear on hard drives in the VOD server.  
4 The content is encrypted real-time with slow changing keys (lasting 20 minutes or  
5 more). For other systems, the VOD content is sent in-the-clear to subscribers.  
6 Storage has been typically in-the-clear or encrypted using a simple "storage key".

7 The frequency and program identifiers (PIDs) used for a VOD session are  
8 privately signaled through encrypted transactions, so that someone trying to  
9 eavesdrop on the VOD communication cannot receive the tuning information for  
10 the program even if the content is sent in-the-clear. In some systems, the  
11 content is scrambled as an IPPV program. The program is therefore "purchased"  
12 as in a broadcast IPPV program. If an eavesdropper could locate the VOD  
13 channel, he or she would still need to pay for the movie as the legitimate  
14 customer.

15 In addition to the security provided by encryption, encryption of PIDs and  
16 frequencies and other measures, VOD security also relies on the fact that both  
17 the content and viewing times are under control of a legitimate purchasing party.  
18 That party can pause the program for a half an hour or all day. The content can  
19 be "rewound" or started over from scratch. These factors all contribute to  
20 providing protection against pirating of the content.

21 For all of the differences between VOD programming and conventional  
22 programming for cable and satellite programming, there remains a significant  
23 problem when a cable or satellite operator wishes to utilize decoder equipment  
24 (e.g., television set top boxes (STBs)) from multiple vendors. As with  
25 conventional cable television, each vendor generally uses its own conditional  
26 access (CA) encryption system. If a multiple service operator (MSO) chooses to  
27 utilize multiple STBs in a system, it must somehow accommodate multiple CA  
28 systems. This problem has been discussed extensively in the above-referenced  
29 patent applications. Since VOD content storage is limited, duplicating content so

1 that it may be available to both legacy and non-legacy CAs may not be a  
2 practical (because of a lack of rack space), or economical (storage costs money).

3

4

#### BRIEF DESCRIPTION OF THE DRAWINGS

5 The features of the invention believed to be novel are set forth with  
6 particularity in the appended claims. The invention itself however, both as to  
7 organization and method of operation, together with objects and advantages  
8 thereof, may be best understood by reference to the following detailed  
9 description of the invention, which describes certain exemplary embodiments of  
10 the invention, taken in conjunction with the accompanying drawings in which:

11 **FIGURE 1** is a block diagram of an exemplary video on demand cable  
12 television system consistent with certain embodiments of the present invention.

13 **FIGURE 2** is a flow chart depicting operation of an exemplary embodiment  
14 consistent with certain embodiments of the present invention.

15 **FIGURE 3** illustrates conversion from clear content to dual selectively  
16 encrypted content to single selectively encrypted content in a manner consistent  
17 with certain embodiments of the present invention.

18 **FIGURE 4** is a block diagram of an exemplary video on demand server  
19 consistent with certain embodiments of the present invention.

20

21

#### DETAILED DESCRIPTION OF THE INVENTION

22 While this invention is susceptible of embodiment in many different forms,  
23 there is shown in the drawings and will herein be described in detail specific  
24 embodiments, with the understanding that the present disclosure is to be  
25 considered as an example of the principles of the invention and not intended to  
26 limit the invention to the specific embodiments shown and described. In the  
27 description below, like reference numerals are used to describe the same, similar  
28 or corresponding parts in the several views of the drawings.

1       The terms “scramble” and “encrypt” and variations thereof are used  
2 synonymously herein. The term “video” may be used herein to embrace not only  
3 true visual information, but also in the conversational sense (e.g., “video tape  
4 recorder”) to embrace not only video signals but associated audio and data. The  
5 present document generally uses the example of a “dual selective encryption”  
6 embodiment, but those skilled in the art will recognize that the present invention  
7 can be utilized to realize multiple partial encryption without departing from the  
8 invention. The terms “partial encryption” and “selective encryption” are used  
9 synonymously herein. Also, the terms “program” and “television program” and  
10 similar terms can be interpreted in the normal conversational sense, as well as a  
11 meaning wherein the term means any segment of A/V content that can be  
12 displayed on a television set or similar monitor device. The term “legacy” as  
13 used herein refers to existing technology used for existing cable and satellite  
14 systems. The exemplary embodiments disclosed herein are decoded by a  
15 television Set-Top Box (STB), but it is contemplated that such technology will  
16 soon be incorporated within television receivers of all types whether housed in a  
17 separate enclosure alone or in conjunction with recording and/or playback  
18 equipment or Conditional Access (CA) decryption module or within a television  
19 set itself. The present document generally uses the example of a “dual partial  
20 encryption” embodiment, but those skilled in the art will recognize that the  
21 present invention can be utilized to realize multiple partial encryption without  
22 departing from the invention.

23       The above-referenced commonly owned patent applications describe  
24 inventions relating to various aspects of methods generally referred to herein as  
25 partial encryption or selective encryption. More particularly, systems are  
26 described wherein selected portions of a particular selection of digital content  
27 are encrypted using two (or more) encryption techniques while other portions of  
28 the content are left unencrypted. By properly selecting the portions to be  
29 encrypted, the content can effectively be encrypted for use under multiple

1 decryption systems without the necessity of encryption of the entire selection of  
2 content. In some embodiments, only a few percent of data overhead is needed  
3 to effectively encrypt the content using multiple encryption systems. This results  
4 in a cable or satellite system being able to utilize Set-top boxes or other  
5 implementations of conditional access (CA) receivers from multiple  
6 manufacturers in a single system - thus freeing the cable or satellite company to  
7 competitively shop for providers of Set-top boxes.

8       The present invention applies similar selective encryption techniques to  
9 the problem of multiple VOD encryption systems. The partial encryption  
10 processes described in the above patent applications utilize any suitable  
11 encryption method. However, these encryption techniques are selectively  
12 applied to the data stream, rather than encrypting the entire data stream, using  
13 techniques described in the above-referenced patent applications. In general,  
14 but without the intent to be limiting, the selective encryption process utilizes  
15 intelligent selection of information to encrypt so that the entire program does not  
16 have to undergo dual encryption. By appropriate selection of data to encrypt, the  
17 program material can be effectively scrambled and hidden from those who desire  
18 to hack into the system and illegally recover commercial content without paying.  
19 MPEG (or similar format) data that are used to represent the audio and video  
20 data does so using a high degree of reliance on the redundancy of information  
21 from frame to frame. Certain data can be transmitted as "anchor" data  
22 representing chrominance and luminance data. That data is then often simply  
23 moved about the screen to generate subsequent frames by sending motion  
24 vectors that describe the movement of the block. Changes in the chrominance  
25 and luminance data are also encoded as changes rather than a recoding of  
26 absolute anchor data. Thus, encryption of this anchor data, for example, or other  
27 key data can effectively render the video un-viewable.

28       In accordance with certain embodiments consistent with the present  
29 invention, the selected video data to be encrypted may be any individual one or



1 combination of the following (described in greater detail in the above  
2 applications): video slice headers appearing in an active region of a video frame,  
3 data representing an active region of a video frame, data in a star pattern within  
4 the video frame, data representing scene changes, I Frame packets, packets  
5 containing motion vectors in a first P frame following an I Frame, packets having  
6 an intra\_slice\_flag indicator set, packets having an intra\_slice indicator set,  
7 packets containing an intra\_coded macroblock, data for a slice containing an  
8 intra\_coded macroblock, data from a first macroblock following the video slice  
9 header, packets containing video slice headers, anchor data, and P Frame data  
10 for progressively refreshed video data, data arranged in vertical and or horizontal  
11 moat patterns on the video frame, and any other selected data that renders the  
12 video and/or audio difficult to utilize. Several such techniques as well as others  
13 are disclosed in the above-referenced patent applications, any of which (or other  
14 techniques) can be utilized with the present invention to encrypt only a portion of  
15 the content.

16 Referring now to **FIGURE 1**, a VOD content delivery system 100  
17 consistent with certain embodiments of the present invention is illustrated. In this  
18 system, a cable television multiple services operator (MSO) operates a cable  
19 head end 104 to provide content to subscribers. VOD content is statically stored  
20 on VOD servers such as servers 108 and 112 depicted as located at cable hubs  
21 116 and 120 respectively. The VOD content is delivered to a specific  
22 subscriber's STB such as STB 124, 128, 132 or 136 upon receipt of a specific  
23 request by that subscriber.

24 In accordance with certain embodiments consistent with the present  
25 invention, content stored in the VOD servers is delivered to the ordering STB  
26 which has an individual identification code that can be addressed by the cable  
27 head end and VOD server. Because VOD is interactive, the cable system can  
28 learn not only the address of the ordering STB, but also what type of STB the

1 ordering STB is (e.g., a legacy or non-legacy set-top box), and what CA system  
2 the STB uses.

3 Using selective encryption for subscription and IPPV broadcast services  
4 as described in the above-referenced patent applications, cable operators can  
5 manage content in real-time - received and decrypted off HITS satellites, and  
6 then selectively re-encrypted for the legacy and non-legacy conditional access  
7 (CA) providers operating in the cable plant. Such selective encryption entails  
8 duplicating and encrypting certain important or critical segments of the content  
9 independently with each CA while sending the remainder of the content in the  
10 clear. The clear content can be received by both legacy and non-legacy set-top  
11 boxes, affording a huge savings in bandwidth from the "full dual carriage"  
12 approach, while the encrypted content is decrypted by the respective set-top  
13 boxes with the particular CA.

14 In VOD systems, since the content is directed to a specific target STB (the  
15 ordering STB), the efficiency of both transmission and storage of the content can  
16 be enhanced using multiple and single selective encryption in accordance with  
17 embodiments consistent with the present invention. **FIGURE 2** depicts a process  
18 200 consistent with an embodiment of the present invention starting at 202 in  
19 which the VOD content is stored as a multiple (e.g., dual) selectively encrypted  
20 content and then transmitted as single selectively encrypted content. At 206, the  
21 content is selectively multiply encrypted. This is carried out by selecting  
22 appropriate segments of content to be encrypted that are important or critical to  
23 the decoding of the content, duplicating those selected segments content and  
24 encrypting each copy using a different encryption method (one for each CA  
25 system in use). The resulting multiple selectively encrypted content is then  
26 stored on the VOD server(s) or at a data repository in the cable head end. Of  
27 course, those skilled in the art will understand that any time critical PCR  
28 information should be fixed along with the Continuity Counter information in the  
29 duplicated packets.

1           When VOD content is ordered by a subscriber at 214, the cable system  
2 (e.g., using registration information stored at the cable head end for each STB)  
3 determines what type of STB is associated with the order and thus what type of  
4 CA encryption system is being used by the ordering STB at 218. Once this is  
5 determined, there is no need to transmit the multiple selectively encrypted  
6 content to the subscriber (unless the order somehow is to be associated with  
7 multiple STBs of different types as in a household having two different STBs,  
8 both of which are to be entitled to decode the content). Thus, the encrypted  
9 portions of the content that are encrypted under a CA encryption not used by the  
10 ordering STB are stripped out at 222 to convert the multiple selectively encrypted  
11 VOD content into single selectively encrypted VOD content. The remaining  
12 encrypted content is then associated with the program identifier used by the clear  
13 unencrypted content to produce the single selectively encrypted VOD content.  
14 This single selectively encrypted VOD content is then provided to the ordering  
15 STB at 226. As a result of the order of the VOD content, a bill is ultimately sent  
16 to the subscriber at 230 for the VOD content and the process ends at 234.

17           Thus, in accordance with certain embodiments consistent with the present  
18 invention, a video on demand (VOD) method, involves storing multiple selective  
19 encrypted VOD content on a VOD server; receiving an order for the VOD content  
20 specifying delivery to a target decoder; determining what CA encryption system  
21 is associated with the order; stripping all encrypted segments from the multiple  
22 selectively encrypted content that are not associated with the order to produce  
23 single selectively encrypted VOD content; and sending the single selectively  
24 encrypted VOD content to the target decoder. The multiple selectively encrypted  
25 VOD content can be created by examining unencrypted data representing digital  
26 content to identify segments of content for encryption; encrypting the identified  
27 segments of content using a first encryption method associated with a first  
28 conditional access system to produce first encrypted segments; encrypting the  
29 identified segments of content using a second encryption method associated with

1 a second conditional access system to produce second encrypted segments; and  
2 replacing the identified segments of content with the first encrypted content and  
3 the second encrypted content in the digital content, to produce the multiple  
4 selectively encrypted VOD content.

5 The data streams or files representing the VOD content associated with  
6 this process are depicted in **FIGURE 3**. The clear content is represented by  
7 packets or other segments of data containing a "C" while encrypted segments  
8 encrypted under CA encryption system A is represented by the designations  
9 "CA-A". Encrypted segments encrypted under CA encryption system B is  
10 represented by designations "CA-B". The initial file is either unencrypted or  
11 decrypted and its initial 16 segments is shown as 310. In order to produce the  
12 multiply selectively encrypted file, in this case dual selectively encrypted,  
13 segments 7 and 14 are selected for encryption. These segments may  
14 correspond to important or critical data needed for decoding or may be selected  
15 according to any desired selection criteria. These segments are duplicated,  
16 encrypted under CA-A and CA-B and reinserted into the file or data stream as  
17 shown to produce the dual selectively encrypted file. This file 320 can then be  
18 stored for later retrieval, when a customer places an order for this VOD content,  
19 on one or more of the VOD servers at the cable hubs or at the cable head end.  
20 Once an order is placed, and the order is associated with a particular type of STB  
21 (the target STB or ordering STB) and thus a particular type of CA encryption, the  
22 dual selectively encrypted content is converted to single encrypted content for  
23 transmission to the ordering STB. This is done by stripping out the unneeded  
24 portions that are encrypted under any unused CA systems to produce a data  
25 stream such as that depicted in 330. In this case, CA-A encrypted segments are  
26 stripped out and CA-B encrypted segments remain.

27 Thus, by use of this technique the storage requirements of the VOD file  
28 servers are minimized by not requiring full multiple copies of encrypted content to  
29 be stored thereon. Still, the content is stored in a secure manner with low

1 overhead needed to accommodate the multiple encryption schemes. The  
2 content, when sent to the ordering STB is further optimized to eliminate the small  
3 amount of overhead used for the second CA encryption scheme to further  
4 enhance the efficiency of the utilization of the bandwidth for transmission of the  
5 VOD content to the ordering STB. Since the VOD system knows which set-top  
6 box, legacy or non-legacy, it is sending content to, the content does not need to  
7 be sent with packet duplication. This can preserve bandwidth on the cable plant.  
8 While the elimination of the un-needed packet is not strictly required, it provides  
9 the advantage of minimizing bandwidth and can eliminate the need for a  
10 "shadow" or secondary PID to be called out in the Program Map Table (PMT) as  
11 described in the above-referenced patent applications, since the encrypted  
12 packet can be mapped to the primary PID associated with the unencrypted  
13 content.

14 The process 200 of **FIGURE 2** can be carried out on any suitable  
15 programmed general purpose processor operating as a VOD server/encoder  
16 such as that depicted as computer 400 of **FIGURE 4**. Computer 400 has one or  
17 more central processor units (CPU) 410 with one or more associated buses 414  
18 used to connect the central processor unit 410 to Random Access Memory 418  
19 and Non-Volatile Memory 422 in a known manner. Output devices 426, such as  
20 a display and printer, are provided in order to display and/or print output for the  
21 use of the MSO as well as to provide a user interface such as a Graphical User  
22 Interface (GUI). Similarly, input devices such as keyboard, mouse and  
23 removable media readers 430 may be provided for the input of information by the  
24 operator. Computer 400 also incorporates internal and/or external attached disc  
25 or other mass storage 434 (e.g., disc and/or optical storage) for storing large  
26 amounts of information including, but not limited to, the operating system,  
27 multiple CA encryption methods (if encryption is carried out by the VOD server),  
28 as well as the VOD content (which is most likely stored on massive attached  
29 storage). The Computer system 400 also has an interface 438 for connection to

1 the cable system to service customer requests for content, and may also have  
2 interface 444 that interfaces to multiple encryption devices if the encryption is  
3 carried out by separate hardware. While depicted as a single computer, the  
4 digital content provider may utilize multiple linked computers to carry out the  
5 functions described herein.

6 In one embodiment of an electronic storage medium storing selectively  
7 encrypted video on demand (VOD) programming consistent with embodiments of  
8 the invention, stores a file representing multiple selective encrypted VOD content  
9 having: segments of unencrypted VOD content; first encrypted segments of VOD  
10 content encrypted using a first encryption method associated with a first  
11 conditional access system; second encrypted segments of VOD content  
12 encrypted using a second encryption method associated with a second  
13 conditional access system;  
14 the first and second encrypted segments of VOD content representing the same  
15 segment of VOD content when not encrypted. A first segment of code, when  
16 executed operates to remove one of the first and second encrypted segments of  
17 VOD content from the multiple selective encrypted VOD content to produce  
18 single selectively encrypted content for transmission to a target decoder. The  
19 first segment of code operates to remove one of the first and second encrypted  
20 segments of VOD content upon receipt of an order for the VOD content  
21 specifying delivery to a target decoder, and upon determining which CA  
22 encryption system is associated with the order. The second segment of code  
23 sends the single selectively encrypted VOD content to the target decoder. A  
24 third segment of code associates a program identifier with the single selectively  
25 encrypted VOD content, wherein the same PIDs are used for encrypted and  
26 unencrypted segments of content.

27 Those skilled in the art will recognize that the present invention has been  
28 described in terms of exemplary embodiments based upon use of a programmed  
29 processor (e.g., computer 400). However, the invention should not be so limited,

1 since the present invention could be implemented using hardware component  
2 equivalents such as special purpose hardware and/or dedicated processors  
3 which are equivalents to the invention as described and claimed. Similarly,  
4 general purpose computers, microprocessor based computers, micro-controllers,  
5 optical computers, analog computers, dedicated processors and/or dedicated  
6 hard wired logic may be used to construct alternative equivalent embodiments of  
7 the present invention. Moreover, although the present invention has been  
8 described in terms of a general purpose personal computer providing a playback  
9 mechanism, the playback can be carried on a dedicated machine without  
10 departing from the present invention.

11 Those skilled in the art will appreciate that the program steps and  
12 associated data used to implement the embodiments described above can be  
13 implemented using disc storage as well as other forms of storage such as for  
14 example Read Only Memory (ROM) devices, Random Access Memory (RAM)  
15 devices; optical storage elements, magnetic storage elements, magneto-optical  
16 storage elements, flash memory, core memory and/or other equivalent storage  
17 technologies without departing from the present invention. Such alternative  
18 storage devices should be considered equivalents.

19 The present invention, as described in embodiments herein, is  
20 implemented using a programmed processor executing programming instructions  
21 that are broadly described above form that can be stored on any suitable  
22 electronic storage medium or transmitted over any suitable electronic  
23 communication medium or otherwise be present in any computer readable or  
24 propagation medium. However, those skilled in the art will appreciate that the  
25 processes described above can be implemented in any number of variations and  
26 in many suitable programming languages without departing from the present  
27 invention. For example, the order of certain operations carried out can often be  
28 varied, additional operations can be added or operations can be deleted without  
29 departing from the invention. Error trapping can be added and/or enhanced and

1 variations can be made in user interface and information presentation without  
2 departing from the present invention. Such variations are contemplated and  
3 considered equivalent.

4       Software code and/or data embodying certain aspects of the present  
5 invention may be present in any computer readable medium, transmission  
6 medium, storage medium or propagation medium including, but not limited to,  
7 electronic storage devices such as those described above, as well as carrier  
8 waves, electronic signals, data structures (e.g., trees, linked lists, tables, packets,  
9 frames, etc.) optical signals, propagated signals, broadcast signals, transmission  
10 media (e.g., circuit connection, cable, twisted pair, fiber optic cables,  
11 waveguides, antennas, etc.) and other media that stores, carries or passes the  
12 code and/or data. Such media may either store the software code and/or data or  
13 serve to transport the code and/or data from one location to another. In the  
14 present exemplary embodiments, MPEG compliant packets, slices, tables and  
15 other data structures are used, but this should not be considered limiting since  
16 other data structures can similarly be used without departing from the present  
17 invention.

18       While the invention has been described in conjunction with specific  
19 embodiments, it is evident that many alternatives, modifications, permutations  
20 and variations will become apparent to those skilled in the art in light of the  
21 foregoing description. Accordingly, it is intended that the present invention  
22 embrace all such alternatives, modifications and variations as fall within the  
23 scope of the appended claims.

24       What is claimed is:



- 1 1. A video on demand (VOD) method, comprising:
  - 2 storing multiple selective encrypted VOD content on a VOD server;
  - 3 receiving an order for the VOD content specifying delivery to a target
  - 4 decoder;
  - 5 determining what CA encryption system is associated with the order;
  - 6 stripping all encrypted segments from the multiple selectively encrypted
  - 7 content that are not associated with the order to produce single selectively
  - 8 encrypted VOD content; and
  - 9 sending the single selectively encrypted VOD content to the target
  - 10 decoder.
- 11
- 12 2. The method according to claim 1, further comprising:
  - 13 examining unencrypted data representing digital content to identify
  - 14 segments of content for encryption;
  - 15 encrypting the identified segments of content using a first encryption
  - 16 method associated with a first conditional access system to produce first
  - 17 encrypted segments;
  - 18 encrypting the identified segments of content using a second encryption
  - 19 method associated with a second conditional access system to produce second
  - 20 encrypted segments; and
  - 21 replacing the identified segments of content with the first encrypted
  - 22 content and the second encrypted content in the digital content, to produce the
  - 23 multiple selectively encrypted VOD content.
- 24
- 25 3. The method according to claim 1, further comprising associating a
- 26 program identifier with the single selectively encrypted VOD content, wherein the
- 27 same PIDs are used for encrypted and unencrypted segments of content.
- 28

1 4. The method according to claim 1, wherein the decoder comprises a  
2 television Set-top box.

3

4 5. The method according to claim 1, wherein the VOD server resides at a  
5 cable hub.

6

7 6. A computer readable medium storing instructions which, when executed  
8 on a programmed processor, carry out the VOD method according to claim 1.

9

10 7. An electronic transmission medium carrying single selectively encrypted  
11 VOD content created by the method according to claim 1.

1 8. A video on demand (VOD) method, comprising:  
2 examining unencrypted data representing digital content to identify  
3 segments of content for encryption;  
4 encrypting the identified segments of content using a first encryption  
5 method associated with a first conditional access system to produce first  
6 encrypted segments;  
7 encrypting the identified segments of content using a second encryption  
8 method associated with a second conditional access system to produce second  
9 encrypted segments;  
10 replacing the identified segments of content with the first encrypted  
11 content and the second encrypted content in the digital content, to produce the  
12 multiple selectively encrypted VOD content;  
13 storing the multiple selective encrypted VOD content on a VOD server  
14 residing at a cable hub;  
15 receiving an order for the VOD content specifying delivery to a target  
16 decoder;  
17 determining what CA encryption system is associated with the order;  
18 stripping all encrypted segments from the multiple selectively encrypted  
19 content that are not associated with the order to produce single selectively  
20 encrypted VOD content;  
21 associating a program identifier with the single selectively encrypted VOD  
22 content, wherein the same PIDs are used for encrypted and unencrypted  
23 segments of content; and  
24 sending the single selectively encrypted VOD content to the target  
25 decoder.  
26

- 1 9. A video on demand (VOD) encoder, comprising:  
2 a programmed processor that examines unencrypted data representing  
3 digital content to identify segments of content for encryption;  
4 a first encrypter that encrypts the identified segments of content using a  
5 first encryption method associated with a first conditional access system to  
6 produce first encrypted segments;  
7 a second encrypter that encrypts the identified segments of content using  
8 a second encryption method associated with a second conditional access system  
9 to produce second encrypted segments;  
10 wherein the programmed processor further receives the first and second  
11 encrypted segments and replacing the identified segments of content with the  
12 first encrypted content and the second encrypted content in the digital content, to  
13 produce the multiple selectively encrypted VOD content;  
14 means for storing the multiple selective encrypted VOD content;  
15 means for receiving an order for the VOD content specifying delivery to a  
16 target decoder;  
17 means for determining what CA encryption system is associated with the  
18 order; and  
19 wherein the programmed processor strips all encrypted segments from the  
20 multiple selectively encrypted content that are not associated with the order to  
21 produce single selectively encrypted VOD content.  
22
- 23 10. The encoder according to claim 9, wherein the programmed processor  
24 further associates a program identifier with the single selectively encrypted VOD  
25 content, wherein the same PIDs are used for encrypted and unencrypted  
26 segments of content, and sends the single selectively encrypted VOD content to  
27 the target decoder.  
28

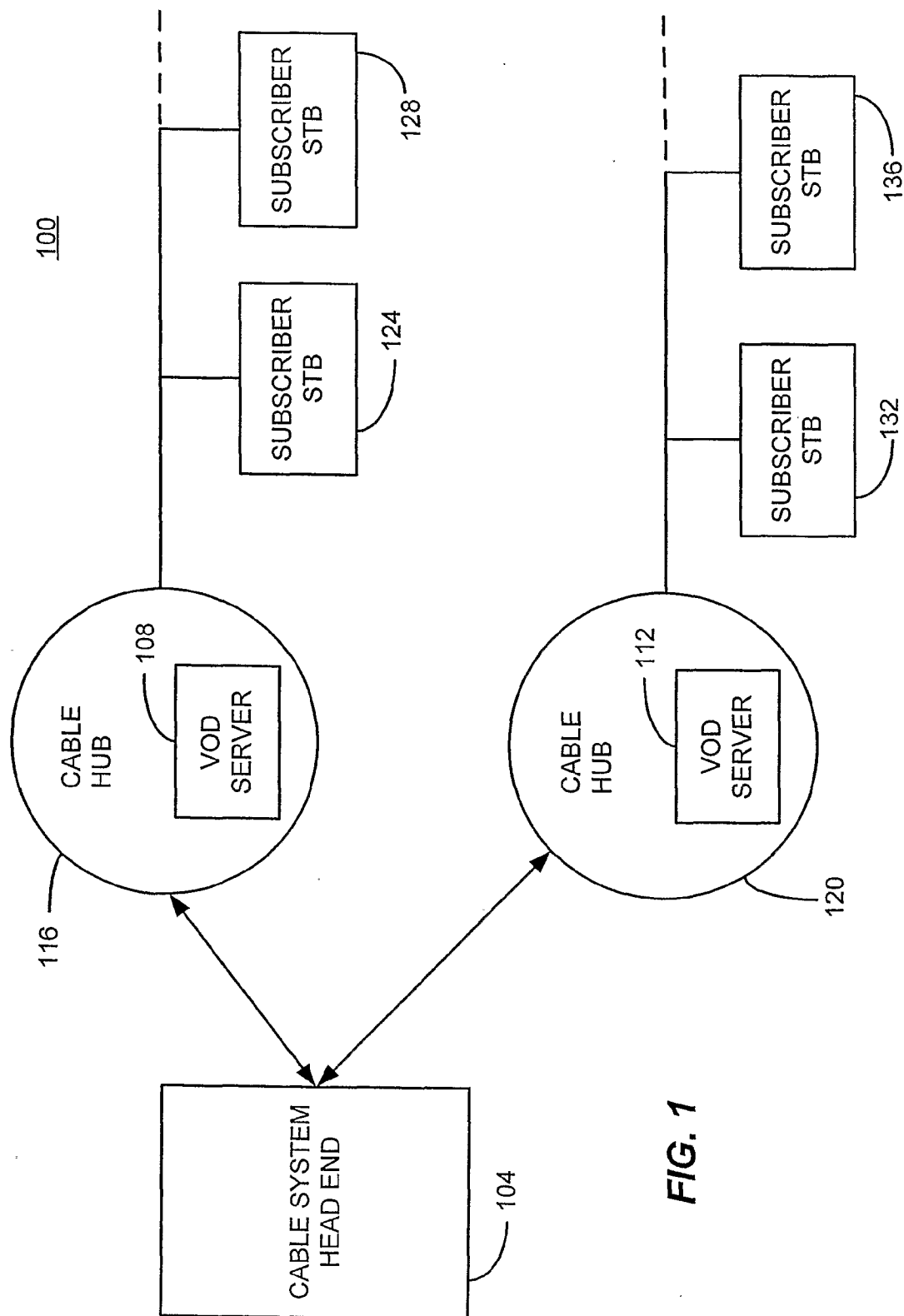
- 1  
2 11. A selectively encrypted video on demand (VOD) system, comprising:  
3 a VOD server storing multiple selective encrypted VOD content;  
4 program means running on a programmed processor for receiving an  
5 order for the VOD content specifying delivery to a target decoder, and for  
6 determining a CA encryption system associated with the order;  
7 wherein, in response to the order, the VOD server strips all encrypted  
8 segments from the multiple selectively encrypted content that are not associated  
9 with the order to produce single selectively encrypted VOD content;  
10 a target decoder addressable by the VOD server; and  
11 means for sending the single selectively encrypted VOD content from the  
12 VOD server to the target decoder.  
13
- 14 12. The system according to claim 11, wherein:  
15 the VOD server carries out a programmed process that examines  
16 unencrypted data representing digital content to identify segments of content for  
17 encryption;  
18 and further comprising:  
19 a first encrypter that encrypts the identified segments of content using a  
20 first encryption method associated with a first conditional access system to  
21 produce first encrypted segments;  
22 a second encrypter that encrypts the identified segments of content using  
23 a second encryption method associated with a second conditional access system  
24 to produce second encrypted segments; and  
25 wherein the VOD server replaces the identified segments of content with  
26 the first encrypted content and the second encrypted content in the digital  
27 content, to produce the multiple selectively encrypted VOD content.  
28

- 1 13. The system according to claim 12, wherein the VOD server further  
2 associates a program identifier with the single selectively encrypted VOD  
3 content, wherein the same PIDs are used for encrypted and unencrypted  
4 segments of content.  
5
- 6 14. The system according to claim 11, wherein the decoder comprises a  
7 television Set-top box.  
8
- 9 15. The system according to claim 11, wherein the VOD server resides at a  
10 cable hub.  
11
- 12 16. The system according to claim 11, wherein the VOD server resides at a  
13 cable system head end.  
14  
15  
16  
17  
18

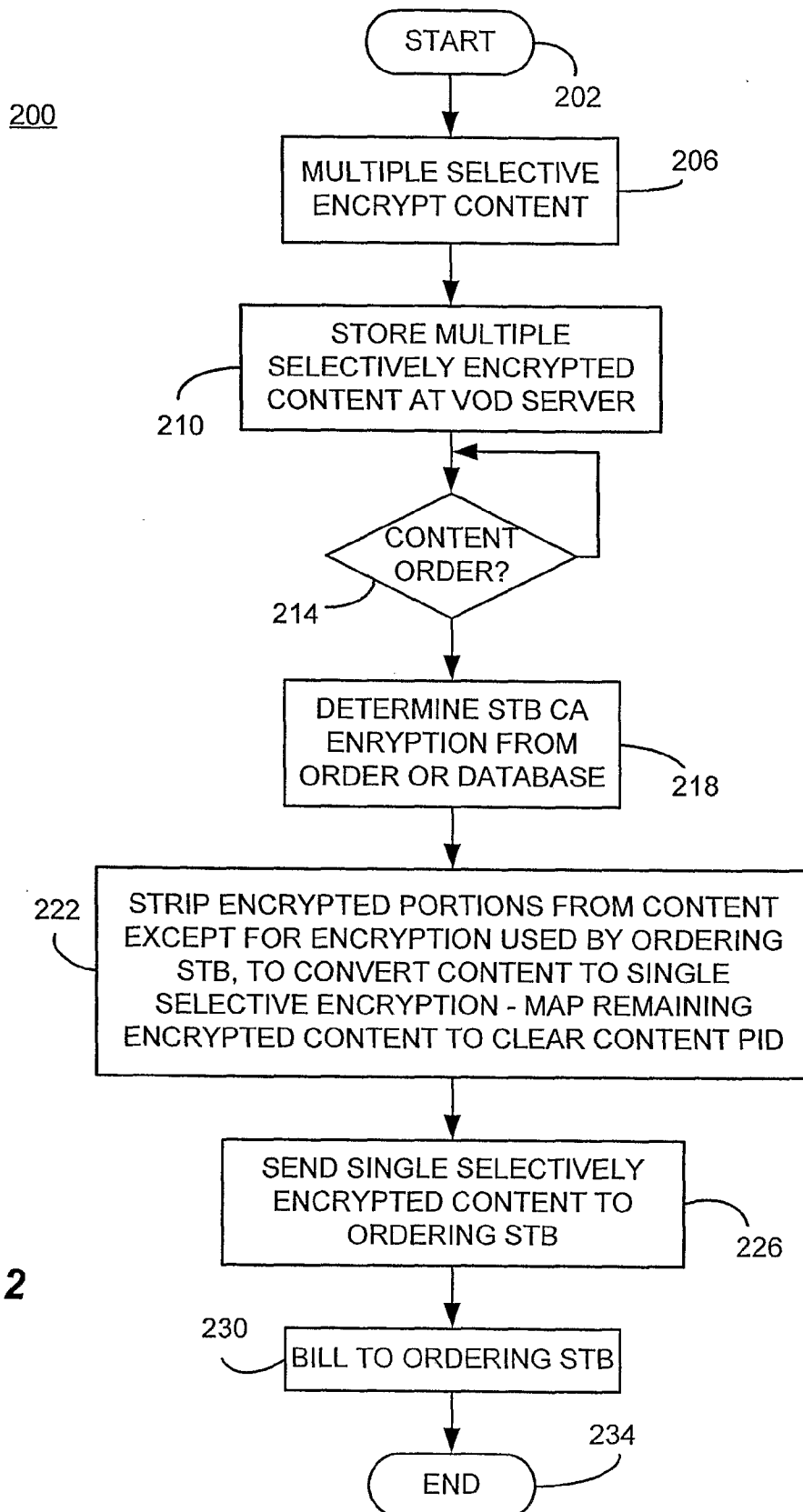
- 1 17. An electronic storage medium storing selectively encrypted video on  
2 demand (VOD) programming, comprising:  
3 a file representing multiple selective encrypted VOD content comprising:  
4 segments of unencrypted VOD content;  
5 first encrypted segments of VOD content encrypted using a first  
6 encryption method associated with a first conditional access system;  
7 second encrypted segments of VOD content encrypted using a  
8 second encryption method associated with a second conditional access  
9 system;  
10 the first and second encrypted segments of VOD content  
11 representing the same segment of VOD content when not encrypted;  
12 a first segment of code that when executed operates to remove one of the  
13 first and second encrypted segments of VOD content from the multiple selective  
14 encrypted VOD content to produce single selectively encrypted content for  
15 transmission to a target decoder.  
16
- 17 18. The electronic storage medium according to claim 17, wherein the first  
18 segment of code operates to remove one of the first and second encrypted  
19 segments of VOD content upon receipt of an order for the VOD content  
20 specifying delivery to a target decoder, and upon determining which CA  
21 encryption system is associated with the order.  
22
- 23 19. The electronic storage medium according to claim 17, further comprising a  
24 second segment of code that sends the single selectively encrypted VOD content  
25 to the target decoder.

1 20. The electronic storage medium according to claim 17, further comprising a  
2 third segment of code that associates a program identifier with the single  
3 selectively encrypted VOD content, wherein the same PIDs are used for  
4 encrypted and unencrypted segments of content.  
5





**FIG. 1**

**FIG. 2**

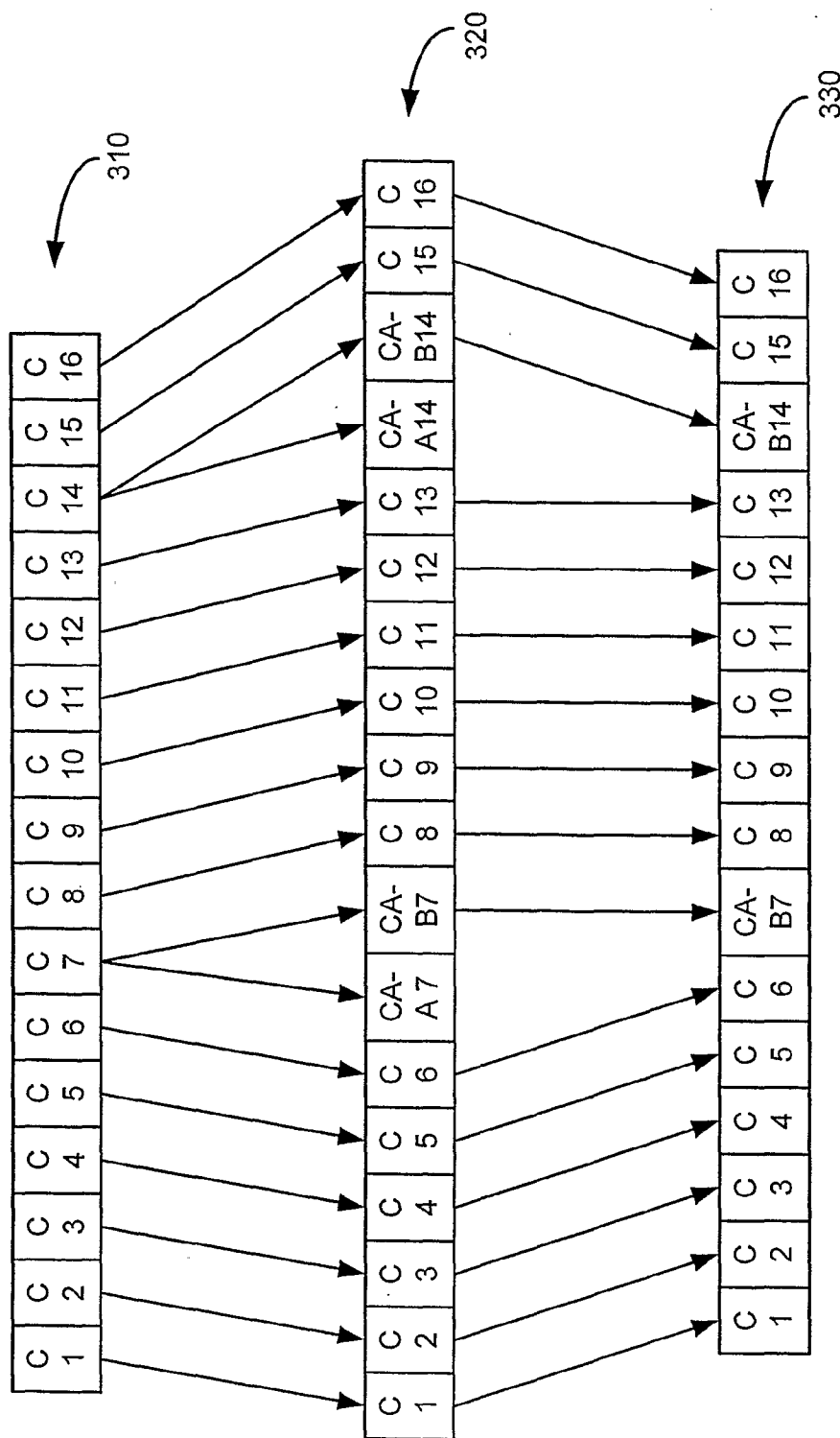
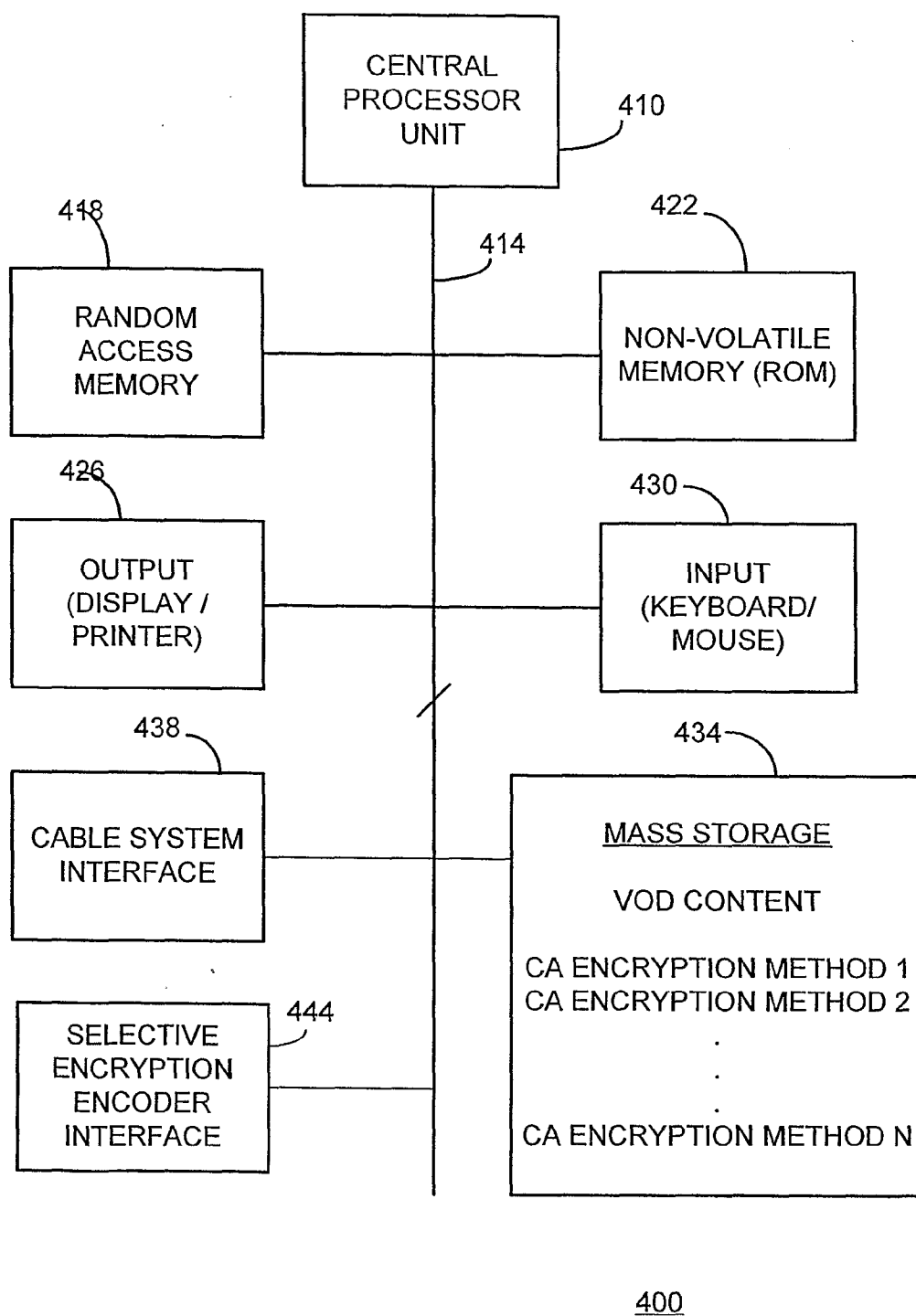


FIG. 3

**FIG. 4**